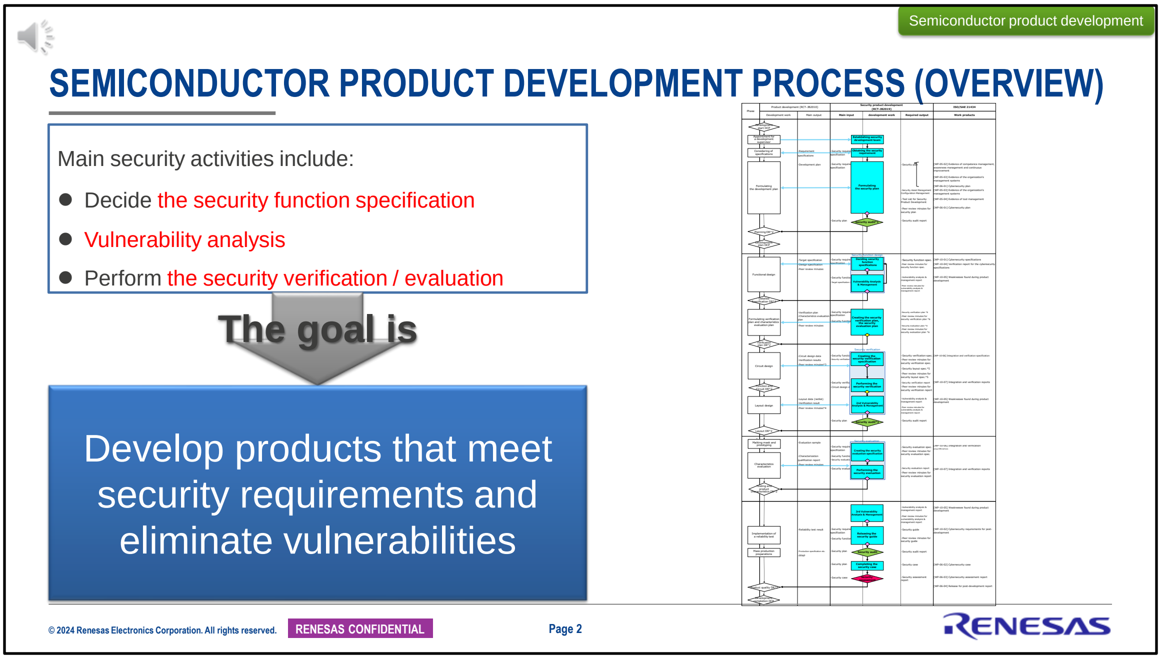
2. SEMICONDUCTOR PRODUCT DEVELOPMENT

This video is a lecture video about the semiconductor product development process, which is part of the security product development process.



Semiconductor product development

SEMICONDUCTOR PRODUCT DEVELOPMENT PROCESS (OVERVIEW)

Main security activities include:

- Decide the security function specification
- Vulnerability analysis
- Perform the security verification / evaluation

The goal is

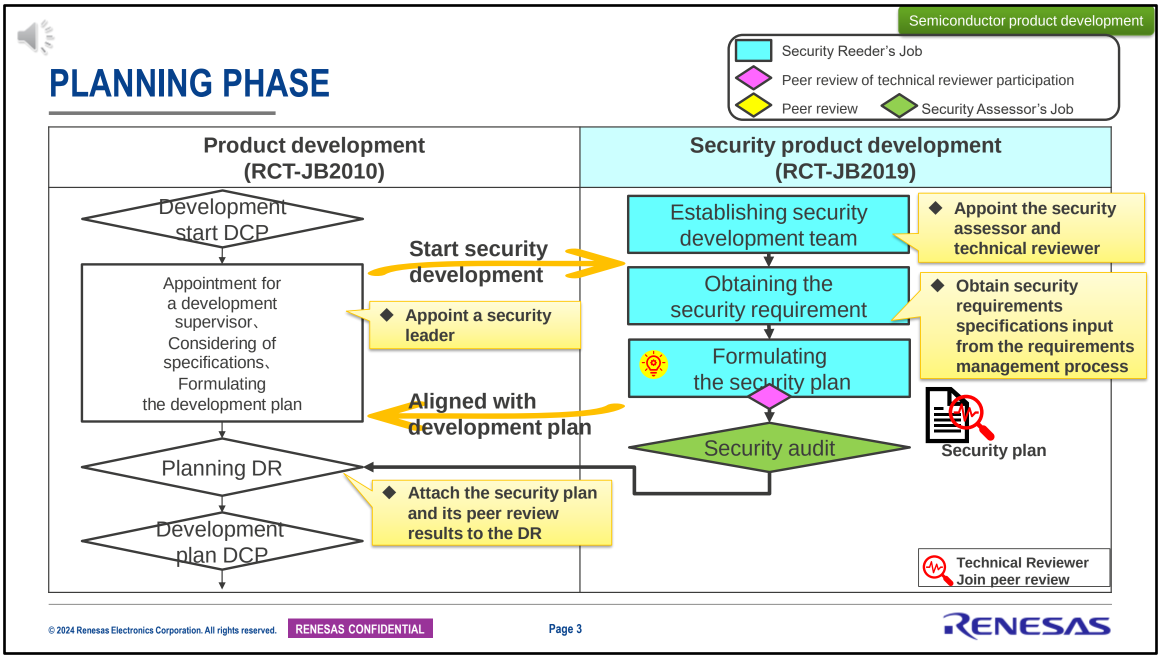
Develop products that meet security requirements and eliminate vulnerabilities

RENESAS CONFIDENTIAL

Page 2

Semiconductor product development process, overview.
On the right is a security colorful chart of the semiconductor product development process.
The light blue squares represent security activities added for security response, the green diamonds represent security audits, and the red diamonds represent security assessments.
The main activities in developing security-enabled semiconductor products include determining security function specifications, vulnerability analysis and management, and security verification and evaluation.
The goal of these activities is to develop products that meet the security requirements input from the requirements management process and eliminate vulnerabilities.

From the next page, I will explain the security development process while comparing it with the QM development process.



Semiconductor product development

PLANNING PHASE

🟦	Security Reeder’s Job
◆	Peer review of technical reviewer participation
◆	Peer review
◆	Security Assessor’s Job

Product development (RCT-JB2010)

Development start DCP

Appointment for a development supervisor、Considering of specifications、Formulating the development plan

Planning DR

Development plan DCP

Start security development

- **Appoint a security leader**

Aligned with development plan

- **Attach the security plan and its peer review results to the DR**

Security product development (RCT-JB2019)

Establishing security development team

- **Appoint the security assessor and technical reviewer**

Obtaining the security requirement

- **Obtain security requirements specifications input from the requirements management process**

Formulating the security plan

Security audit

Security plan

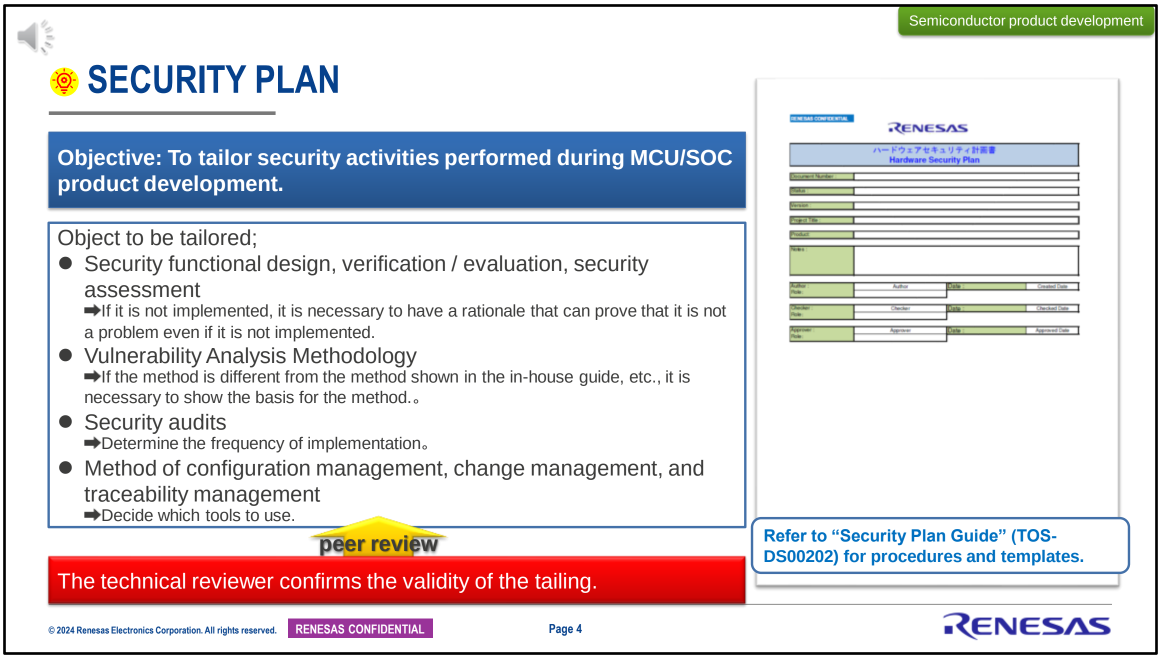
Technical Reviewer Join peer review

RENESAS CONFIDENTIAL

RENESAS

This is the planning phase.
The left side shows the development process of RCT-JB2010, a QM standard, and the right side shows the development flow of RCT-JB2019, which defines security activities.
Development start DCP is held in accordance with RCT-JB2010, and the formulation of a development plan begin.
After the development supervisor is appointed, the development supervisor appoints a security leader. A security leader is appointed and security development begins. In other words, the security development flow on the right side starts.
The development supervisor builds the security development system by asking the appropriate department to select security assessors and technical reviewers.
The security leader obtains the security requirements specification output from the requirements management process.
We plan security activities while taking product development plans into consideration.
The security plan is explained on the next page.
We conducts a peer review of the developed security plan. This peer

review requires the participation of a technical reviewer, as shown in pink diamond.
After the findings of the peer review of the security plan have been addressed, a security audit is conducted by a security assessor.
In the planning DR specified in RCT-JB2010, the security plan and its peer review results are reported, and agreement is obtained from the DR attendees.
The above is the content to be implemented in the planning phase.
In the planning phase, formulating a plan for activities is the same as QM development. However, the difference from QM development is that the plan is reviewed by a technical reviewer and an audit by a security assessor.



Semiconductor product development

SECURITY PLAN

Objective: To tailor security activities performed during MCU/SOC product development.

Object to be tailored;

- ● Security functional design, verification / evaluation, security assessment
  ➡If it is not implemented, it is necessary to have a rationale that can prove that it is not a problem even if it is not implemented.
- ● Vulnerability Analysis Methodology
  ➡If the method is different from the method shown in the in-house guide, etc., it is necessary to show the basis for the method.。
- ● Security audits
  ➡Determine the frequency of implementation。
- ● Method of configuration management, change management, and traceability management
  ➡Decide which tools to use.

peer review

The technical reviewer confirms the validity of the tailing.

RENESAS CONFIDENTIAL

RENESAS

ハードウェアセキュリティ計画書
Hardware Security Plan

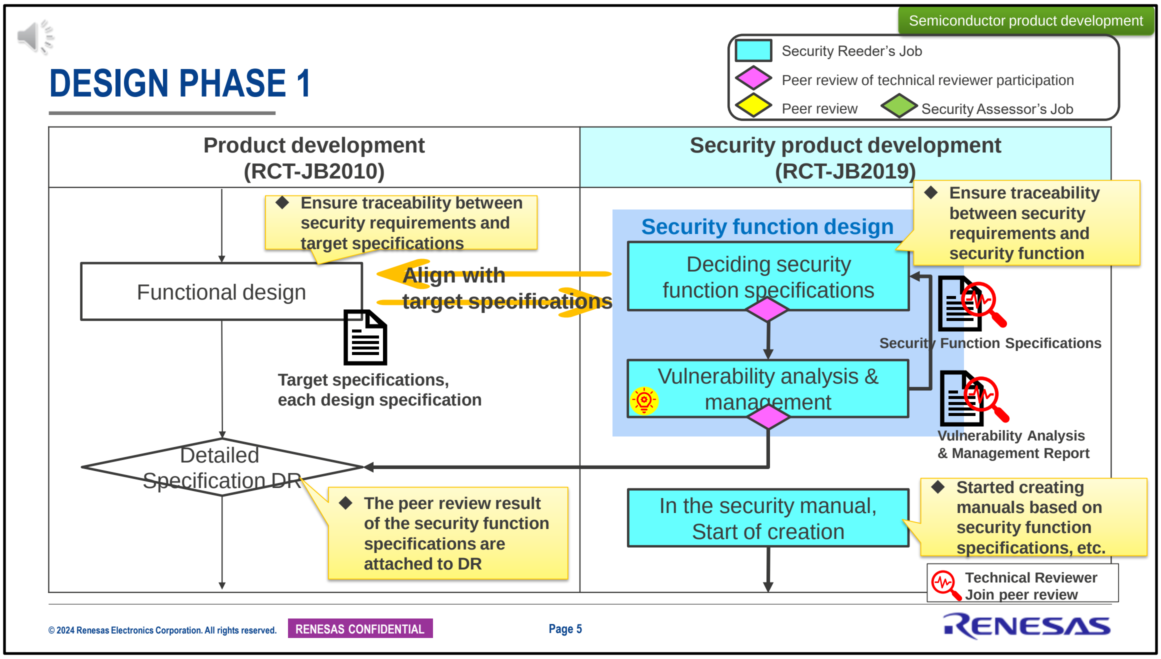
Document Number :			
Status :			
Version :			
Project Title :			
Product :			
Notes :			
Author : Role :	Author	Date :	Created Date
Checker : Role :	Checker	Date :	Checked Date
Approver : Role :	Approver	Date :	Approved Date

Refer to "Security Plan Guide" (TOS-DS00202) for procedures and templates.

© 2024 Renesas Electronics Corporation. All rights reserved. RENESAS CONFIDENTIAL Page 4

RENESAS

Security plan.
The purpose is to tailor the security activities carried out during product development.
There are four things to be tailored: Security function design, verification, evaluation, security assessment.　Vulnerability analysis method. Security audit.　Methods for configuration management, change management and traceability management.
The first to third steps are most likely carried out according to in-house procedures, so I think there is little opportunity for them to be tailored.
Regarding configuration management, RCT-JB2019-002 requires the use of tools, so it is necessary to decide which tools to use for configuration management and how to manage the configuration using the tools.
The security plan containing the results of these tailoring is peer reviewed with the participation of technical reviewers to confirm the validity of the tailoring.
For the procedure and format for creating a security plan, please refer to the Security Plan Guide, TOS-DS00202.



Semiconductor product development

DESIGN PHASE 1

🟦 Security Reeder's Job
◆ Peer review of technical reviewer participation
◆ Peer review ◆ Security Assessor's Job

Product development (RCT-JB2010)	Security product development (RCT-JB2019)

- Ensure traceability between security requirements and target specifications

Functional design

Align with target specifications

Target specifications, each design specification

Detailed Specification DR

- The peer review result of the security function specifications are attached to DR

Security function design

Deciding security function specifications

Vulnerability analysis & management

- Ensure traceability between security requirements and security function

Security Function Specifications

Vulnerability Analysis & Management Report

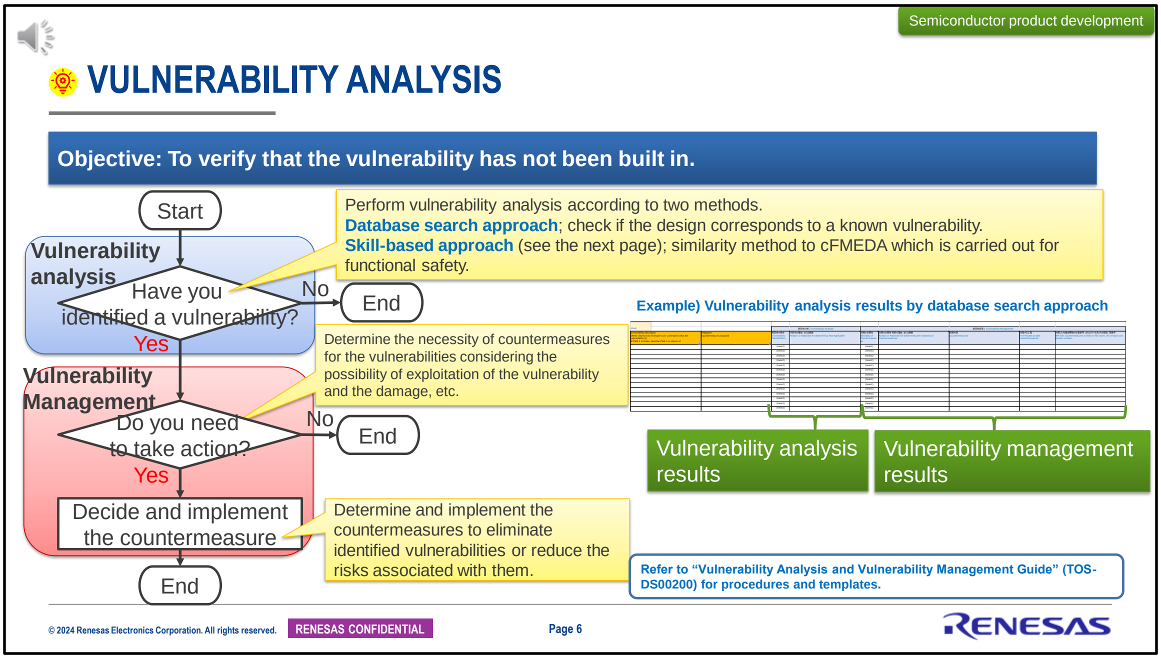
In the security manual, Start of creation

- Started creating manuals based on security function specifications, etc.

Technical Reviewer Join peer review

© 2024 Renesas Electronics Corporation. All rights reserved. RENESAS CONFIDENTIAL Page 5

Design phase.
We perform functional design according to RCT-JB2010.
At this time, security activities include determining security function specifications, and vulnerability analysis and management.
Security function specifications are determined based on the security requirements specifications output as a result of the requirements management process.
Vulnerability analysis is then performed based on the target specifications and security function specifications. Reflect the results of vulnerability analysis in security function specifications and target specifications. As a result of the analysis, if changes such as adding security requirements are required, we make changes to the security requirements specification.
Security functional specifications and vulnerability analysis management reports are peer reviewed with the participation of technical reviewers. We share those results with D R.
The next page describes vulnerability analysis management.



Semiconductor product development

VULNERABILITY ANALYSIS

Objective: To verify that the vulnerability has not been built in.

Start
Vulnerability analysis
Have you identified a vulnerability?
No
End
Yes
Vulnerability Management
Do you need to take action?
No
End
Yes
Decide and implement the countermeasure
End
Vulnerability analysis results
Vulnerability management results

Perform vulnerability analysis according to two methods.
Database search approach; check if the design corresponds to a known vulnerability.
Skill-based approach (see the next page); similarity method to cFMEDA which is carried out for functional safety.

Determine the necessity of countermeasures for the vulnerabilities considering the possibility of exploitation of the vulnerability and the damage, etc.

Determine and implement the countermeasures to eliminate identified vulnerabilities or reduce the risks associated with them.

Example) Vulnerability analysis results by database search approach

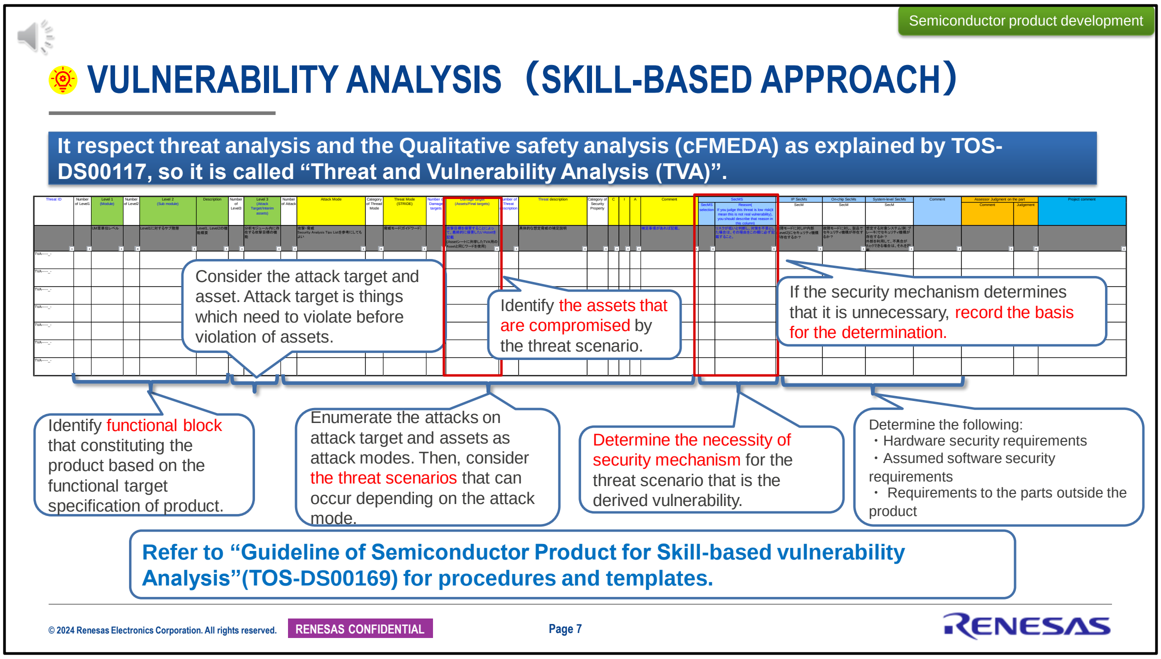
Refer to "Vulnerability Analysis and Vulnerability Management Guide" (TOS-DS00200) for procedures and templates.

RENESAS CONFIDENTIAL Page 6 RENESAS

Vulnerability analysis.
The purpose is to analyze the design specifications and confirm that no vulnerabilities have been created.
I will explain it according to the flow diagram on the left. First, perform vulnerability analysis to identify vulnerabilities.
There are two approaches to vulnerability analysis performed in semiconductor product development.
One is a database search approach. This refers to a vulnerability database maintained by the security technology department to ensure that no known vulnerabilities have been created.
For procedures and forms, please refer to the Vulnerability Analysis and Vulnerability Management Guide, TOS-DS00200.
The second is a skills-based approach. As explained on the next page, this method is similar to the concept F M E D A used for functional safety.

If vulnerability analysis is performed and vulnerabilities are identified, vulnerability management is required.
Decide whether countermeasures are required and record the results

of implementing the countermeasures.
Vulnerability analysis and vulnerability management are thus performed as a set during the development process.
As an example, we have posted the format of a vulnerability analysis management report using a database search approach.
This report also allows you to record both vulnerability analysis results and vulnerability management results.
Vulnerability management is covered in part 4, the management process.



Semiconductor product development

VULNERABILITY ANALYSIS（SKILL-BASED APPROACH）

It respect threat analysis and the Qualitative safety analysis (cFMEDA) as explained by TOS-DS00117, so it is called “Threat and Vulnerability Analysis (TVA)”.

Threat ID	Number of Level1	Level 1 (Module)	Number of Level2	Level 2 (Sub module)	Description	Number of Level3	Level 3 (Attack Target/Interim assets)	Number of Attack	Attack Mode	Category of Thread Mode	Threat Mode (STRIDE)	Number of Damage targets	Damage target (Assets/Final targets)	Number of Threat description	Threat description	Category of Security Property	C	I	A	Comment	SecMS		IP SecMs	On-chip SecMs	System-level SecMs	Comment	Assessor Judgment on the part		Project comment
																					SecMS selection	Reason(If you judge this threat is low risk(it mean this is not real vulnerability), you should describe that reason in this column)	SecM	SecM	SecM		Comment	Judgement	
		UM章単位レベル		Level1に対するサブ階層	Level1, Level2の機能概要		分析モジュール内に存在する攻撃目標の機能		攻撃・脅威 Security Analysis Tips Listを参考にしてもよい		脅威モード(ガイドワード)		攻撃目標を侵害することによって、最終的に侵害したいAssetを記載 (Assetシートに列挙したTVA用のAssetと同じワードを使用)		具体的な想定脅威の補足説明					補足事項があれば記載。		リスクが低いと判断し、対策を不要とした場合は、その理由をこの欄に必ず記載すること。	故障モードに対しIP内部(Level2)にセキュリティ機構が存在するか？	故障モードに対し、製品でセキュリティ機構が存在するか？	想定する対象システム(例:ブレーキ)でセキュリティ機構が存在するか？ 外部を利用して、不具合がﾁｪｯｸできる場合は、それを記載。				
TVA-----_-																													
TVA-----_-																													
TVA-----_-																													
TVA-----_-																													
TVA-----_-																													
TVA-----_-																													
TVA-----_-																													

Consider the attack target and asset. Attack target is things which need to violate before violation of assets.

Identify the assets that are compromised by the threat scenario.

If the security mechanism determines that it is unnecessary, record the basis for the determination.

Identify functional block that constituting the product based on the functional target specification of product.

Enumerate the attacks on attack target and assets as attack modes. Then, consider the threat scenarios that can occur depending on the attack mode.

Determine the necessity of security mechanism for the threat scenario that is the derived vulnerability.

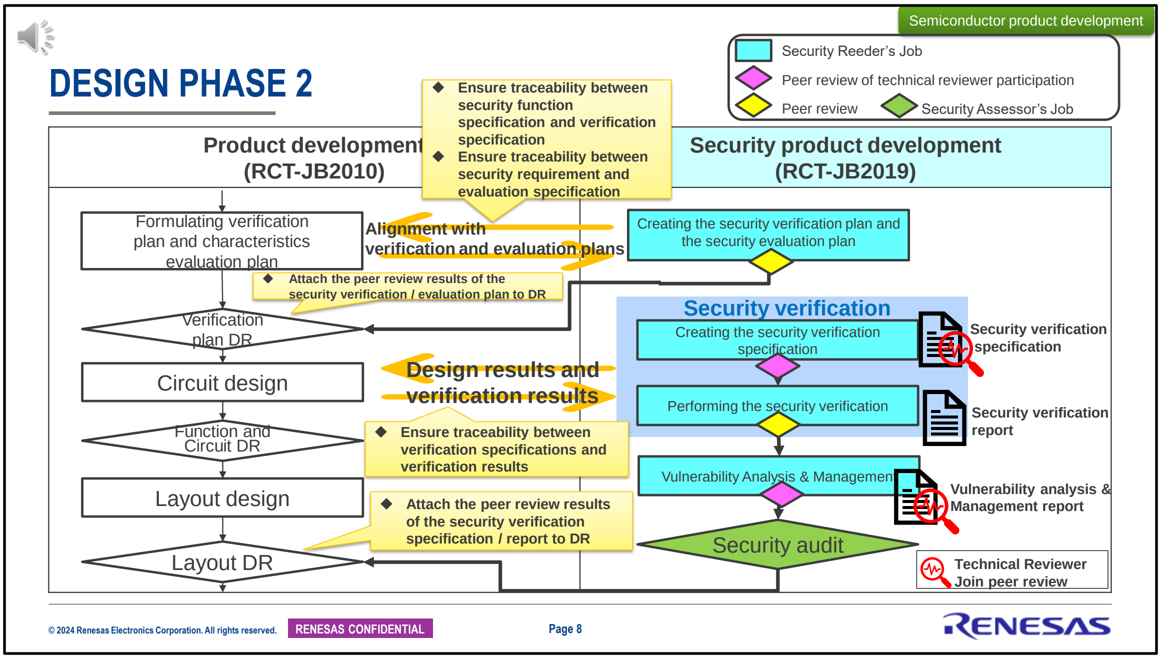
Determine the following:
・Hardware security requirements
・Assumed software security requirements
・ Requirements to the parts outside the product

Refer to “Guideline of Semiconductor Product for Skill-based vulnerability Analysis”(TOS-DS00169) for procedures and templates.

RENESAS CONFIDENTIAL

RENESAS

Vulnerability analysis, skills-based approach.
It also includes threat analysis, so we call it Threat and Vulnerability Analysis, or T V A for short. Here is the format.
By following the step-by-step analysis from left to right, you will be able to identify the necessary security mechanisms.
Enter the functional block on the left side and identify the assets that are likely to be attacked. Then consider threat scenarios that could occur against the asset.
Determine whether security mechanisms are required to counter identified threat scenarios.
A security mechanism is one that is implemented in hardware. It becomes a hardware security requirement. Functions realized by software become software security requirements.
If it is necessary to implement measures other than hardware and software, this will be a request external to the product.
For procedures and formats, refer to the ISO 21434 Skills-Based Vulnerability Analysis Guidelines for Semiconductor Products, TOS-DS00169.



Semiconductor product development

DESIGN PHASE 2

🟦 Security Reeder's Job
◆ Peer review of technical reviewer participation
◆ Peer review ◆ Security Assessor's Job

- ◆ Ensure traceability between security function specification and verification specification
- ◆ Ensure traceability between security requirement and evaluation specification

Product development (RCT-JB2010)

Security product development (RCT-JB2019)

Formulating verification plan and characteristics evaluation plan

Alignment with verification and evaluation plans

Creating the security verification plan and the security evaluation plan

- ◆ Attach the peer review results of the security verification / evaluation plan to DR

Verification plan DR

Security verification

Creating the security verification specification

Security verification specification

Circuit design

Design results and verification results

Performing the security verification

Security verification report

Function and Circuit DR

- ◆ Ensure traceability between verification specifications and verification results

Vulnerability Analysis & Management

Vulnerability analysis & Management report

Layout design

- ◆ Attach the peer review results of the security verification specification / report to DR

Security audit

Layout DR

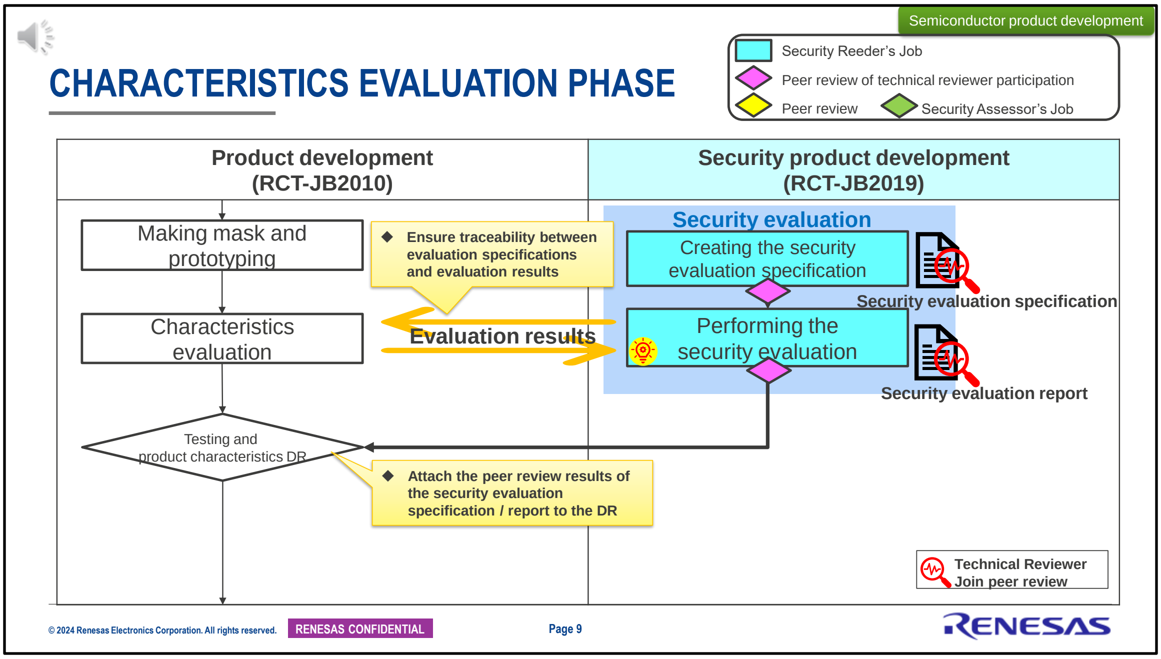
Technical Reviewer Join peer review

RENESAS CONFIDENTIAL Page 8

Also, let's return to the explanation of flow diagrams.
This is a continuation of the design phase. We formulate a verification plan and evaluation plan in accordance with RCT-JB2010.
Similarly, for security, we formulate a security verification plan and a security evaluation plan. The results of the peer review is reported to D R.
Next, circuit design and layout design are performed. During security development, security verification is performed on design results.
Now, create a security verification specification for performing security verification. This security verification specification is subject to peer review with the participation of technical reviewers.
In this design phase, it is important to manage the traceability of specifications such as between functional specifications and verification specifications, or between verification specifications and verification results.
After the peer review of the security verification report is completed, we conduct the second vulnerability analysis.
If the vulnerability database has been updated since the vulnerability analysis performed during function design, analysis is performed on

the newly added vulnerability information.
Even if the vulnerability database has not been updated, we record in the vulnerability analysis management report that analysis will not be performed because there has been no update.
After the second vulnerability analysis management, a security audit is conducted by a security assessor.
Peer review results of security verification specifications and security verification reports are reported in D R.

This concludes the explanation of the security activities to be carried out during the design phase. There were three differences from QM activities.
One is to conduct vulnerability analysis.
Second, technical reviewers must participate in peer reviews of security function specifications, vulnerability analysis management reports, and security verification specifications.
Third, an audit is conducted by a security assessor.



Semiconductor product development

CHARACTERISTICS EVALUATION PHASE

🟦 Security Reeder’s Job
◆ Peer review of technical reviewer participation
◆ Peer review ◆ Security Assessor’s Job

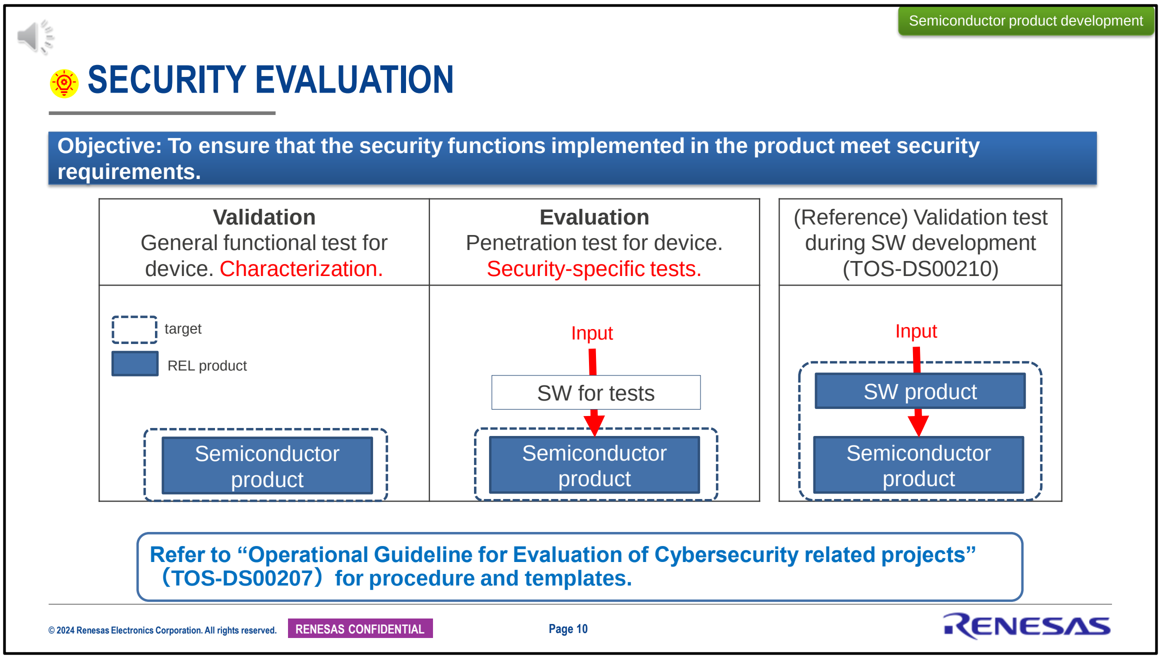
Product development
(RCT-JB2010)
Security product development
(RCT-JB2019)
Making mask and prototyping
Characteristics evaluation
Testing and product characteristics DR
Security evaluation
Creating the security evaluation specification
Performing the security evaluation
Security evaluation specification
Security evaluation report
Evaluation results
Technical Reviewer
Join peer review

- Ensure traceability between evaluation specifications and evaluation results
- Attach the peer review results of the security evaluation specification / report to the DR

© 2024 Renesas Electronics Corporation. All rights reserved. RENESAS CONFIDENTIAL Page 9

RENESAS

Characterization phase.
Characterization is performed according to RCT-JB2010. Security evaluations are also performed during security development.
For security evaluation, in order to perform a security-specific evaluation, we conduct a peer review with the participation of technical reviewers on both the security evaluation specification and the security evaluation report.
The results of peer review of security evaluation specifications and security evaluation reports are reported to the testing and product characteristics D R.
Security evaluation is explained on the next page.



Semiconductor product development

SECURITY EVALUATION

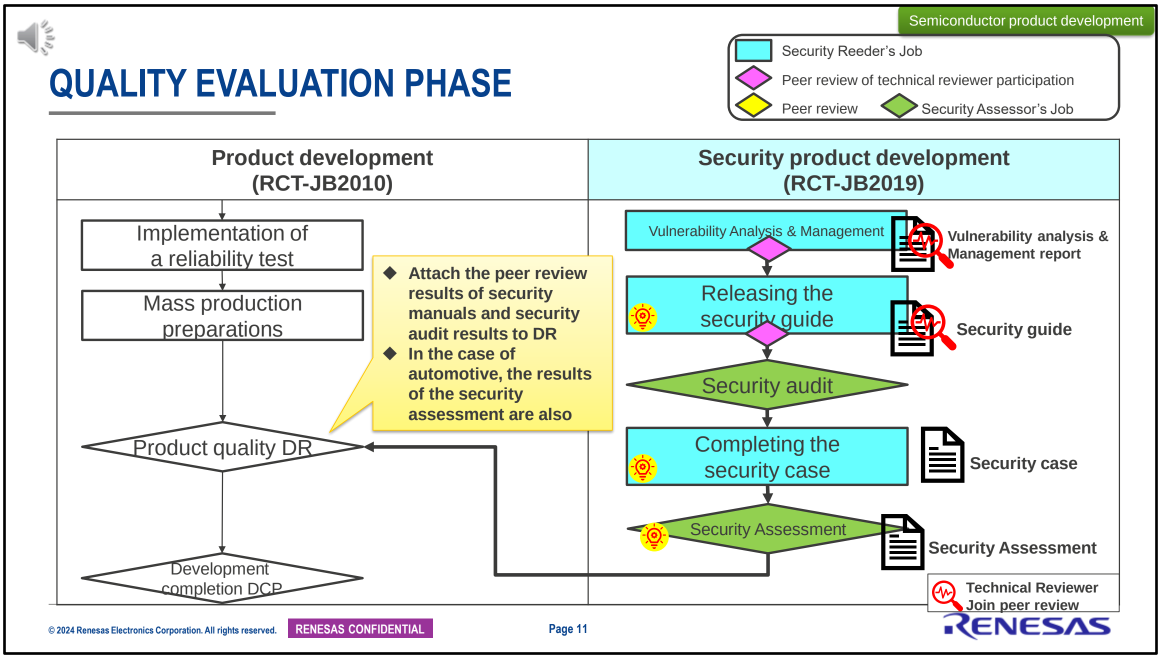
Objective: To ensure that the security functions implemented in the product meet security requirements.

Validation General functional test for device. Characterization.	**Evaluation** Penetration test for device. Security-specific tests.	(Reference) Validation test during SW development (TOS-DS00210)

Refer to "Operational Guideline for Evaluation of Cybersecurity related projects" （TOS-DS00207） for procedure and templates.

Security evaluation.
The purpose of security evaluation is to confirm that the security features implemented in the product meet security requirements. For procedures and formats, please refer to TOS-DS00207, the security evaluation guideline.
In this guide, security evaluation in hardware development is classified into two types: validation and evaluation.
Validation refers to the normal functional testing and characterization of a device. Regarding security functions, we confirm that they are implemented according to specifications using the evaluation items we perform in normal characteristic evaluations.
Another evaluation, this one is a security specific test. Evaluation software is implemented on the semiconductor product to be evaluated, and tests are performed to attempt penetration using known technology from outside to confirm that the product is resistant to cyber attacks. A picture of the software validation test is also posted on the right for reference. In software security validation testing, software products developed on top of semiconductor products are implemented and evaluated.

At this time, the device used for evaluation is equivalent to E S products.



Semiconductor product development

QUALITY EVALUATION PHASE

🟦 Security Reeder's Job
◆ Peer review of technical reviewer participation
◆ Peer review ◆ Security Assessor's Job

Product development
(RCT-JB2010)
Security product development
(RCT-JB2019)
Implementation of a reliability test
Mass production preparations
Product quality DR
Development completion DCP
Vulnerability Analysis & Management
Releasing the security guide
Security audit
Completing the security case
Security Assessment
Vulnerability analysis & Management report
Security guide
Security case
Security Assessment
Technical Reviewer Join peer review

- Attach the peer review results of security manuals and security audit results to DR
- In the case of automotive, the results of the security assessment are also

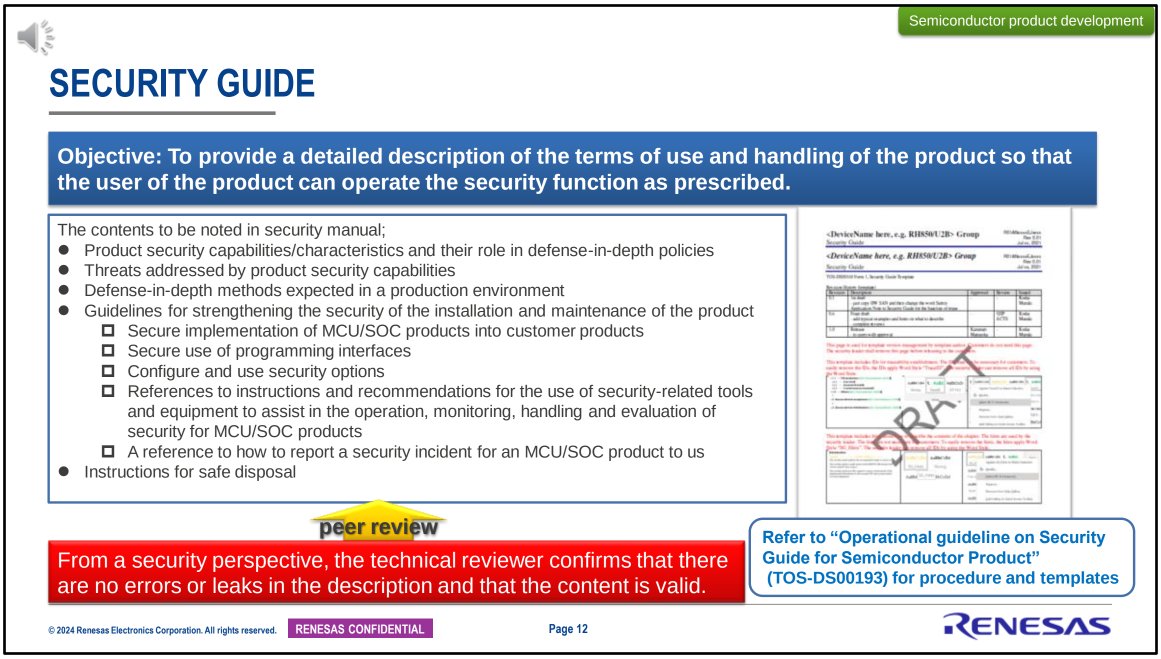
RENESAS CONFIDENTIAL Page 11 RENESAS

Also, let's return to the explanation of flow diagrams. Finally, there is the quality evaluation phase.
Reliability tests and mass production preparations are conducted in accordance with RCT-JB2010.
We conduct the third vulnerability analysis. As with the second vulnerability analysis, we first check for updates to the vulnerability database.
When the vulnerability database is updated, we analyze the newly added vulnerability information.
In order to request countermeasures on the software or customer set side if a vulnerability is identified and countermeasures are required, it is specified that a final vulnerability analysis during development be performed before the release of the security guide.
We conduct a peer review with the participation of technical reviewers for the security guide that we have started creating after designing the security functions.
After releasing the completed security guide, we conduct a security audit by a security assessor. The security leader then confirms that the planned work products have been completed and completes the

security case.
Submit the security case to a security assessor for a security assessment. The security activities are completed by reporting those results to D R.

The above are the security activities carried out in the quality evaluation phase.
Completing a security case and performing a security assessment is not required for industrial or consumer products and are activities specific to automotive products.

The following pages explain the security guide, security case, and security assessment.



Semiconductor product development

SECURITY GUIDE

Objective: To provide a detailed description of the terms of use and handling of the product so that the user of the product can operate the security function as prescribed.

The contents to be noted in security manual;

- Product security capabilities/characteristics and their role in defense-in-depth policies
- Threats addressed by product security capabilities
- Defense-in-depth methods expected in a production environment
- Guidelines for strengthening the security of the installation and maintenance of the product
  - □ Secure implementation of MCU/SOC products into customer products
  - □ Secure use of programming interfaces
  - □ Configure and use security options
  - □ References to instructions and recommendations for the use of security-related tools and equipment to assist in the operation, monitoring, handling and evaluation of security for MCU/SOC products
  - □ A reference to how to report a security incident for an MCU/SOC product to us
- Instructions for safe disposal

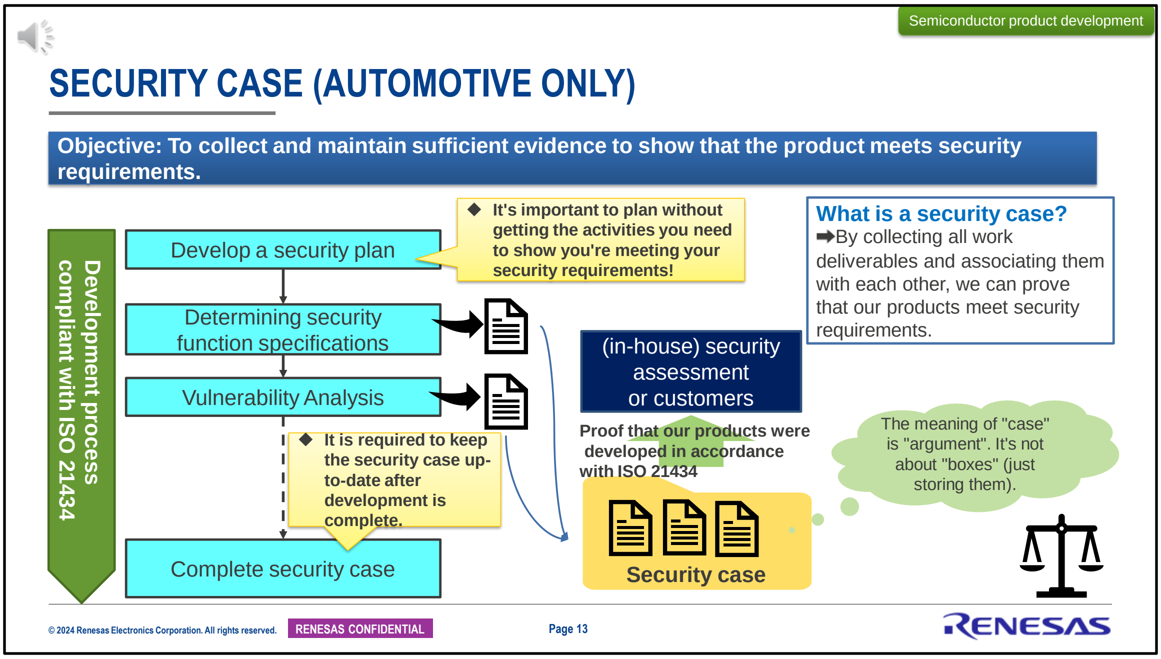
peer review

From a security perspective, the technical reviewer confirms that there are no errors or leaks in the description and that the content is valid.

Refer to "Operational guideline on Security Guide for Semiconductor Product" (TOS-DS00193) for procedure and templates

RENESAS CONFIDENTIAL Page 12 RENESAS

Security guide.
The purpose of creating a security guide is to thoroughly describe the terms of use and handling of the product so that the user of the product can operate the security functions as intended.
The contents of the security guide are as follows.
It is also necessary to implement in the security guide all security guide requirements extracted during the creation of security requirements in the requirements management process, and all the requirements for components external to the product that were derived as a result of T V A conducted during semiconductor product development.
A peer review is conducted on the created security guide with the participation of technical reviewers.
From a security perspective, technical reviewers check that there are no errors or omissions in the descriptions and that the contents are valid.
For the creation procedure and format, please refer to the Operational guideline on Security Guide for Semiconductor Product, TOS-DS00193.



Semiconductor product development

SECURITY CASE (AUTOMOTIVE ONLY)

Objective: To collect and maintain sufficient evidence to show that the product meets security requirements.

Development process compliant with ISO 21434
Develop a security plan
Determining security function specifications
Vulnerability Analysis
Complete security case
(in-house) security assessment or customers
Security case

◆ **It's important to plan without getting the activities you need to show you're meeting your security requirements!**

◆ **It is required to keep the security case up-to-date after development is complete.**

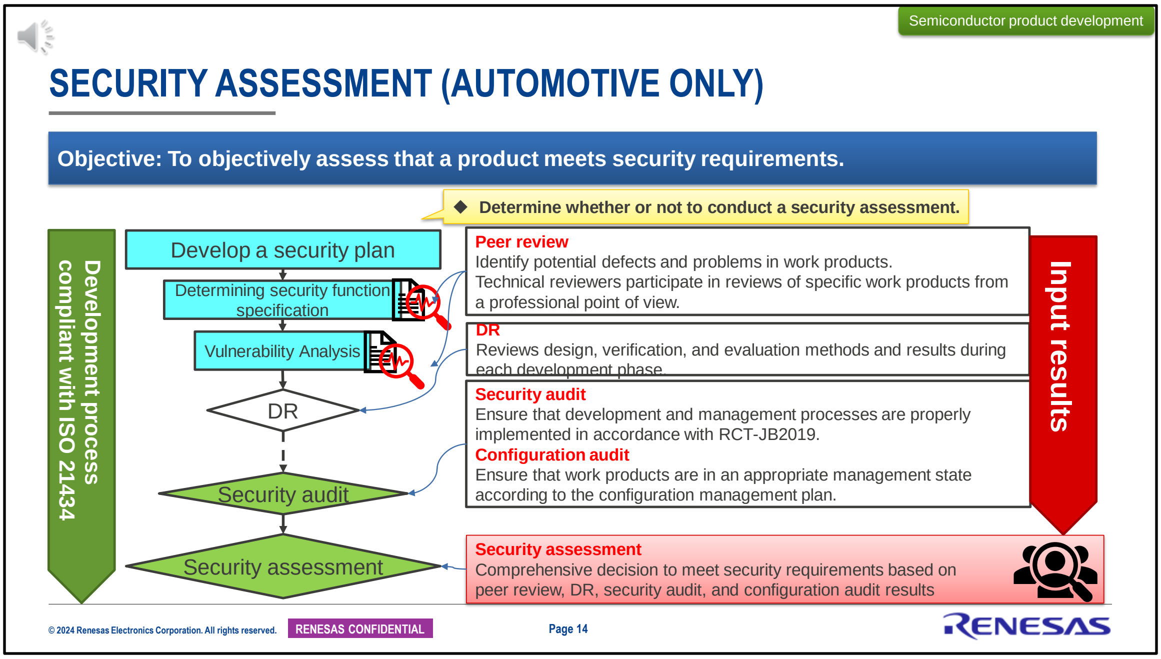
What is a security case?
➡By collecting all work deliverables and associating them with each other, we can prove that our products meet security requirements.

Proof that our products were developed in accordance with ISO 21434

The meaning of "case" is "argument". It's not about "boxes" (just storing them).

© 2024 Renesas Electronics Corporation. All rights reserved. RENESAS CONFIDENTIAL Page 13 RENESAS

Security case.
The purpose is to collect and maintain sufficient evidence to demonstrate that the product meets security requirements.
We develop according to the development process compliant with ISO 21434, that is, RCT-JB2019, and collect the output results one by one and create a security case.
First, when planning, it is important to include all necessary activities in the plan. Otherwise, by the time you finish development and complete your security case, you realize it's not good enough, but it's too late.
When changes are made to a completed security case even after development is complete, it is necessary to update the case and keep it up to date.



Semiconductor product development

SECURITY ASSESSMENT (AUTOMOTIVE ONLY)

Objective: To objectively assess that a product meets security requirements.

◆ Determine whether or not to conduct a security assessment.

Peer review
Identify potential defects and problems in work products.
Technical reviewers participate in reviews of specific work products from a professional point of view.

DR
Reviews design, verification, and evaluation methods and results during each development phase.

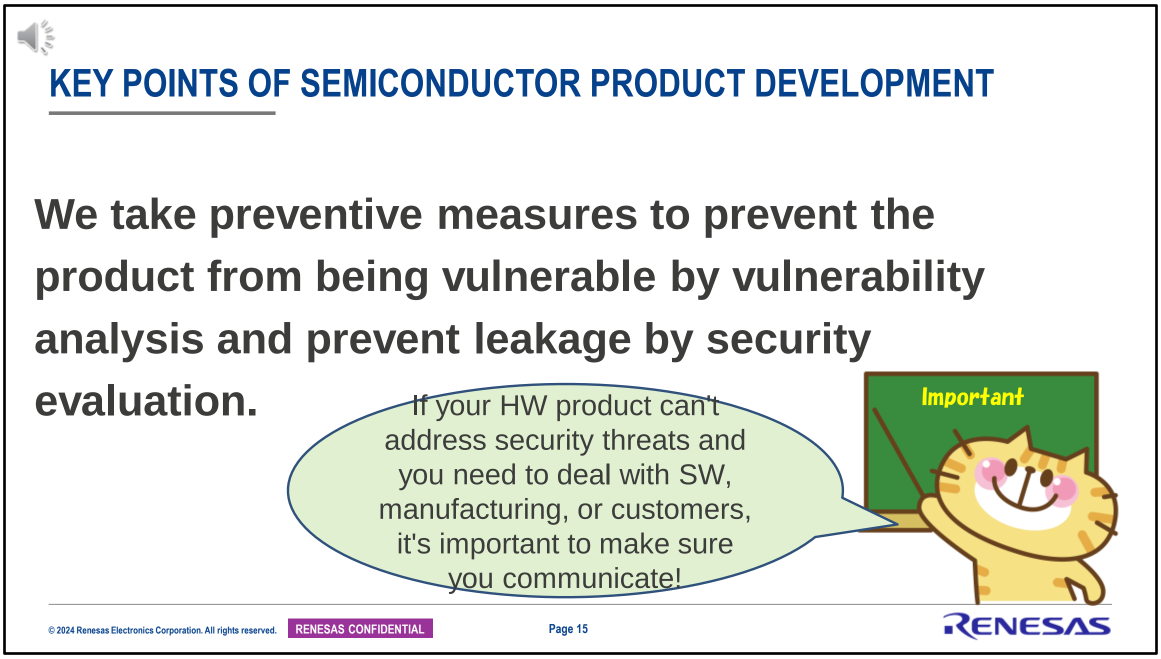
Security audit
Ensure that development and management processes are properly implemented in accordance with RCT-JB2019.

Configuration audit
Ensure that work products are in an appropriate management state according to the configuration management plan.

Security assessment
Comprehensive decision to meet security requirements based on peer review, DR, security audit, and configuration audit results

RENESAS CONFIDENTIAL Page 14 RENESAS

Security assessment.
In a security assessment, a third party objectively evaluates whether a product meets security requirements.
This third party could be a security assessor from the quality department who is independent from the product development team.
We integrate the results of peer reviews, D R, security audits, and configuration audits conducted during product development to determine whether security requirements have been achieved and pass or fail the security assessment.
Security assessments check the results of security activities based on the security cases explained on the previous page.
Security assessment procedures and formats are defined in Procedure of the Security Audit and the security Assessment, TOS-QS00172.
This security assessment report, together with the security guide and security case, are submitted to the customer based on customer agreement. Security assessors also create assessment reports for customer submission.



KEY POINTS OF SEMICONDUCTOR PRODUCT DEVELOPMENT

We take preventive measures to prevent the product from being vulnerable by vulnerability analysis and prevent leakage by security evaluation.

If your HW product can't address security threats and you need to deal with SW, manufacturing, or customers, it's important to make sure you communicate!

RENESAS CONFIDENTIAL Page 15 RENESAS

Key points of semiconductor product development.
We take preventive measures to prevent the product from being vulnerable by vulnerability analysis and prevent leakage by security evaluation.
On the other hand, it is important to describe risks that cannot be addressed by the product in the security guide, communicate them to customers and software developers, and ensure that they are addressed in subsequent processes.

This concludes our explanation of the semiconductor product development process. Thank you for watching.